REMARKS

Applicant provides the present Amendment in response to the Official Action mailed May 23, 2003. Applicants appreciate the indication of allowable subject matter in Claims 23, 24, 26 and 27. Applicants have amended Claims 1 and 22 to recite generating RSA key values for use in encrypting data. Applicants have also written the recitations of Claims 17, 24 and 27 in independent form without including the recitations of intervening claims. Applicants have also added new Claims 28-56 which are system and computer program product claims corresponding to certain of the method dependent Claims 2-21. Applicants submit that these new claims are patentable for reasons analogous to those discussed with reference to Claims 2-21. Applicants have also amended the specification to remove the references to attorney docket numbers.

The IDS

Applicants submit concurrently herewith an Information Disclosure Statement of materials from the related applications.

The Objection to the Specification

Applicants have removed the attorney docket numbers from the Related Applications section of the present specification. Accordingly, Applicants submit that the objection to the specification has been overcome.

The Section § 101 Rejection

Claims 1-22 stand rejected under 35 U.S.C. § 101 as "not within technical art." Official Action, p. 2. Applicants have amended Claims 1 and 22 to recite that cryptographic values p and q are used to generate key values used in encrypting data. Thus, certain embodiments of the present invention provide for specific techniques for generating prime values that are used in the generation of keys used for encryption.

Applicants submit that Claims 1 and 22 are directed to processes that have a practical application in the technological arts. The generation of cryptographic values for use in encrypting data is not a process that merely manipulates an abstract idea or performs a purely mathematical algorithm. Encryption of data utilizing cryptographic keys is clearly a practical

application in the technological arts. For example, Applicants note that United States Patent No. 4,944,007 to Austin has claims directed to "a method of generating key values." Thus, it appears that the Patent Office has previously considered claims directed to generating cryptographic values as including statutory subject matter. Accordingly, Claims 1 and 22, and the claims that depend from Claims 1 and 22, fall within the definition of statutory process claims. *See* Examination Guidelines for Computer-Related Inventions, Final Version, Section IV.B.2(b)(ii), pp. 17-18.

Furthermore, Applicants have amended Claim 16 to place Claim 16 in independent form. Authentication of cryptographic values, as recited in Claim 16, is clearly a useful result and a practical application in the technological arts. Accordingly, Applicants submit that Claim 16 and the claims that depend from Claim 16 recite statutory subject matter.

In light of the above discussion, Applicants submit that Claims 1-22 are directed to statutory subject matter and, therefore, request withdrawal of the present Section 101 rejections.

The Section § 103 Rejections

Claims 1, 2, 3, 11, 12, 22 and 25 stand rejected as obvious under 35 U.S.C. § 103 in light of Rivest et al., "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, Vol. 21, Issue 2, February, 1978 (hereinafter "Rivest") and United States Patent No. 6,215,874 to Borza *et al.* (hereinafter "Borza"). Claim 8 is rejected based on Rivest, Borza and United States Patent No. 6,219,794 to Soutar *et al.* (hereinafter "Soutar").

To establish a prima facie case of obviousness, the prior art reference or references when combined must teach or suggest *all* the recitations of the claims, and there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. M.P.E.P. §2143. The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. M.P.E.P. §2143.01, citing *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990). As emphasized by the Court of Appeals for the Federal Circuit, to support combining references, evidence of a suggestion, teaching, or motivation to

combine must be clear and particular, and this requirement for clear and particular evidence is not met by broad and conclusory statements about the teachings of references. *In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). The Court of Appeals for the Federal Circuit has also stated that, to support combining or modifying references, there must be particular evidence from the prior art as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed. *In re Kotzab*, 55 U.S.P.Q.2d 1313, 1317 (Fed. Cir. 2000). Applicants respectfully submit that such a showing has not been made in this case.

For example, independent Claim 1 recites the following:

1. A method of generating RSA cryptographic values, the method comprising the steps of:

obtaining entity specific information (B) about a user;

obtaining a first secret seed value (W_p) and a second secret seed value (W_q);

obtaining a third, publicly known, randomization value (IV) having a first portion (IV_p) and a second portion (IV_q);

dividing a potential range of RSA encryption values into a first interval and a second interval;

generating a first initial value (XX_p) based on the first secret seed value (W_p), the second secret seed value (W_q) and the first portion of the third randomization value (IV_p);

mapping the first initial value to a entity specific segment of the first interval utilizing the obtained entity specific information (B) to provide a mapped first initial value (X_p);

selecting a first user dependent RSA cryptographic value (p) from the entity specific segment of the first interval utilizing the mapped first initial value as a starting point for a search for the first user dependent RSA cryptographic value;

generating a second initial value (XX_q) based on the first user dependent RSA cryptographic value (p), the second secret seed value (W_q) and the first portion of the third randomization value (IV_q);

mapping the second initial value to a entity specific segment of the second interval utilizing the obtained entity specific information to provide a mapped second initial value (X_q); ~~**and**~~

selecting a second user dependent RSA cryptographic value (q) from the entity specific segment of the second interval utilizing the mapped second initial value as a starting point for a search for the second user dependent RSA cryptographic value; and

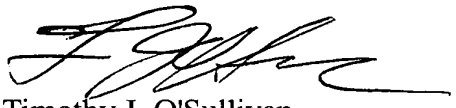
generating an RSA cryptographic key value for use in encrypting data utilizing the first and second user dependent RSA cryptographic values p and q.

Similar recitations are found in Claims 22 and 25. However, the Official Action fails to identify any portion of the cited references that disclose most of the recitations of these claims. As discussed above, to establish a prima facie case of obviousness, each recitation of the claim must be found in the art. The Official Action has not established where any of the highlighted portions of Claim 1 are found in any of the cited references. In fact, the cited Rivest article merely describes the RSA cryptographic algorithm discussed in the Background of the present specification. The cited portions of Borza, likewise, fail to disclose or suggest the details of selection of the p and q cryptographic values as recited in Claim 1. The Section 103 rejection in the Official Action is similarly deficient with reference to Claims 22 and 25. The Official Action, likewise, fails to establish any motivation for combining and/or modifying the cited references to result in the recitations of Claims 1, 22 or 25. As such, Applicants submit that each of the pending claims are patentable over the cited references and, therefore, request withdrawal of the present rejection.

Conclusion

In light of the above discussion, Applicants submit that the present application is in condition for allowance, which action is respectfully requested.

Respectfully submitted,

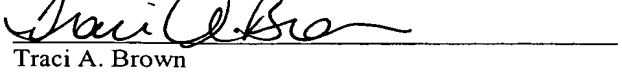


Timothy J. O'Sullivan
Registration No. 35,632

Customer No. 20792
Myers Bigel Sibley & Sajovec
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401

Certificate of Mailing under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450 on August 25, 2003.



Traci A. Brown